PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To: MACRAE & CO. P.O. Box 806 Station B OTTAWA, Ontario Canada, K1P 5T4	**PCT** NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION (PCT Rule 44.1)
	Date of mailing *(day/month/year)* 15 December 2006 (15-12-2006)
Applicant's or agent's file reference 32225	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/CA2006/001562	International filing date *(day/month/year)* 22 September 2006 (22-09-2006)
Applicant ENTRUST LIMITED	

1. [X] The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19 :
   The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46) :

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes
   1211 Geneva 20, Switzerland, Facsimile No.: +41 22 338 82 70

   For more detailed instructions, see the notes on the accompanying sheet.

2. [ ] The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. [ ] **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that :

   [ ] the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

   [ ] no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90*bis*.1 and 90*bis*.3, respectively, before the completion of the technical preparations for the international publication.

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/CA Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001-819-953-2476	Authorized officer Chantal Hébert 819- 953-4957

NOTES TO FROM PCT/ISA/220

These Notes are intended to give instructions concerning the filing of amendments under Article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the *PCT Applicant's Guide*, a publication of WIPO.

In these Notes, "Article," "Rule" and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions, respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report and the written opinion of the International Searching Authority, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims, description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only (see *PCT Applicant's Guide*, Volume I/A, Annexes B1 and B2).

The attention of the applicant is drawn to the fact that amendments to the claims under Article 19 are not allowed where the International Searching Authority has declared, under Article 17(2), that no international search report would be established (see *PCT Applicant's Guide*, Volume I/A, paragraph 296).

What parts of the international application may be amended?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Preliminary Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

When? Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

Where not to file the amendments?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

How? Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet must be submitted for each sheet of the claims which, on account of an amendment or amendments, differs from the sheet originally filed.

All the claims appearing on a replacement sheet must be numbered in Arabic numerals. Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively (Section 205(b)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments?

Letter (Section 205(b)) :

The amendments must be submitted with a letter.
The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").
The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

The letter must indicate the differences between the claims as filed and the claims as amended. It must, in particular, indicate, in connection with each claim appearing in the international application (it being understood that identical indications concerning several claims may be grouped), whether

(i) the claim is unchanged;
(ii) the claim is cancelled;
(iii) the claim is new;
(iv) the claim replaces one or more claims as filed;
(v) the claim is the result of the division of a claim as filed.

The following examples illustrate the manner in which amendments must be explained in the accompanying letter:

1. [Where originally there were 48 claims and after amendment of some claims there are 51]:
"Claims 1 to 29, 31, 32, 34, 35, 37 to 48 replaced by amended claims bearing the same numbers; claims 30, 33 and 36 unchanged; new claims 49 to 51 added."

2. [Where originally there were 15 claims and after amendment of all claims there are 11]:
"Claims 1 to 15 replaced by amended claims 1 to 11."

3. [Where originally there were 14 claims and the amendments consist in cancelling some claims and in adding new claims]:
"Claims 1 to 6 and 14 unchanged; claims 7 to 13 cancelled; new claims 15, 16 and 17 added." or
"Claims 7 to 13 cancelled; new claims 15, 16 and 17 added; all other claims unchanged."

4. [Where various kinds of amendments are made]:
"Claims 1-10 unchanged; claims 11 to 13, 18 and 19 cancelled; claims 14, 15 and 16 replaced by amended claim 14; claim 17 subdivided into amended claims 15, 16 and 17; new claims 20 and 21 added."

"Statement under Article 19(1)" (Rule 46.4)

The amendments may be accompanied by a statement explaining the amendments and indicating any impact that such amendments might have on the description and the drawings (which cannot be amended under Article 19(1)).

The statement will be published with the international application and the amended claims.

It must be in the language in which the international application is to be published.

It must be brief, not exceeding 500 words if in English or if translated into English.

It should not be confused with and does not replace the letter indicating the differences between the claims as filed and as amended. It must be filed on a separate sheet and must be identified as such by a heading, preferably by using the words "Statement under Article 19(1)."

It may not contain any disparaging comments on the international search report or the relevance of citations contained in that report. Reference to citations, relevant to a given claim, contained in the international search report may be made only in connection with an amendment of that claim.

Consequence if a demand for international preliminary examination has already been filed

If, at the time of filing any amendments and any accompanying statement, under Article 19, a demand for international preliminary examination has already been submitted, the applicant must preferably, at the time of filing the amendments (and any statement) with the International Bureau, also file with the International Preliminary Examining Authority a copy of such amendments (and of any statement) and, where required, a translation of such amendments for the procedure before that Authority (see Rules 55.3(a) and 62.2, first sentence). For further information, see the Notes to the demand form (PCT/IPEA/401).

If a demand for international preliminary examination is made, the written opinion of the International Searching Authority will, except in certain cases where the International Preliminary Examining Authority did not act as International Searching Authority and where it has notified the International Bureau under Rule 66.1*bis*(b), be considered to be a written opinion of the International Preliminary Examining Authority. If a demand is made, the applicant may submit to the International Preliminary Examining Authority a reply to the written opinion together, where appropriate, with amendments before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later (Rule 43*bis*.1(c)).

Consequence with regard to translation of the international application for entry into the national phase

The applicant's attention is drawn to the fact that, upon entry into the national phase, a translation of the claims as amended under Article 19 may have to furnished to the designated/elected Offices, instead of, or in addition to, the translation of the claims as filed.

For further details on the requirements of each designated/elected Office, see the *PCT Applicant's Guide*, Volume II.

TENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 32225	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below
International application No. **PCT/CA2006/001562**	International filing date *(day/month/year)* 22 September 2006 (22-09-2006)	(Earliest)Priority date *(day/month/year)* 30 September 2005 (30-09-2005)

Applicant
ENTRUST LIMITED

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 6 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

a. With regard to the **language**, the international search was carried out on the basis of:

[X] the international application in the language in which it was filed

[ ] a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))

b. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I

2. [ ] **Certain claims were found unsearchable** (see Box No. II)

3. [ ] **Unity of invention is lacking** (see Box No. III)

4. With regard to the **title**,

[X] the text is approved as submitted by the applicant

[ ] the text has been established by this Authority to read as follows :

5. With regard to the **abstract**,

[X] the text is approved as submitted by the applicant

[ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings**,

a. the figure of the **drawings** to be published with the abstract is Figure No. 1

[X] as suggested by the applicant

[ ] as selected by this Authority, because the applicant failed to suggest a figure

[ ] as selected by this Authority, because this figure better characterizes the invention

b. [ ] none of the figures is to be published with the abstract

A. CLASSIFICATION OF SUBJECT MATTER
IPC: ***H04L 9/32*** (2006.01)
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC: ***H04L 9/32*** (2006.01) using keywords

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
Delphion, Canadian Patent Database, IEEEXplore, Scholar
Keywords: authentication, challenge, reply, response, password/passphrase, off-line, on-line, mutual, two-factor, zero knowledge

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US4795890; "Device Authentication System for On and Off Line Use"; Goldman, R.; January 3, 1989 (03-01-1989) [col. 2, lines 7-48], [col. 3, lines 7-54], [col. 7, lines 13-29], [Figure 1]	1-78
A	US2005/0033688; "Methods and Apparatus for a Secure Proximity Integrated Circuit Card Transactions"; Peart et al.; February 10, 2005 (10-02-2005) [Abstract], [0017], [0018], [0097], [0103], [0105], [0107]-[0114]	1-78
A	US2005/0144450; "Method and Apparatus for Providing Mutual Authentication Between a Sending Unit and a Recipient"; Voice, C.; June 30, 2005 (30-06-2005) [whole document]	1-78

[ ] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 December 2006 (06-12-2006)	15 December 2006 (15-12-2006)
Name and mailing address of the ISA/CA Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001(819)953-2476	Authorized officer Lawrence J. Engel 819- 997-2936

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US4795890	03-01-1989	NONE	
US2005033688	10-02-2005	AT258328T T	15-02-2004
		AT311634T T	15-12-2005
		AU775976B B2	19-08-2004
		AU781322B B2	19-05-2005
		AU2263501 A	03-07-2001
		AU3287501 A	31-07-2001
		AU4347301 A	17-09-2001
		AU6507801 A	03-12-2001
		AU7090700 A	26-03-2001
		AU7349800 A	10-04-2001
		AU2003248849 A1	23-01-2004
		AU2003259100 A1	23-01-2004
		AU2003265262 A1	23-01-2004
		AU2003287337 A1	03-06-2004
		AU2004216969 A1	16-09-2004
		AU2004231226 A1	23-12-2004
		BR0013822 A	23-07-2002
		BR0014018 A	21-05-2002
		BR0208536 A	14-09-2004
		BR0210962 A	08-06-2004
		BR0304735 A	06-07-2004
		CA2382882 A1	15-03-2001
		CA2382922 A1	08-03-2001
		CA2397722 A1	26-07-2001
		CA2410006 A1	29-11-2001
		CA2442518 A1	10-10-2002
		CA2452351 A1	23-01-2003
		CA2458143 A1	15-01-2004
		CA2518481 A1	16-09-2004
		CN1235175C C	04-01-2006
		CN1376292 A	23-10-2002
		CN1539246 A	20-10-2004
		CN1682222 A	12-10-2005
		CZ20020744 A3	18-02-2004
		CZ20020776 A3	11-09-2002
		DE60007883D D1	26-02-2004
		DK1222620T T3	18-04-2006
		EP1212732 A2	12-06-2002
		EP1222620 A2	17-07-2002
		EP1261945 A2	04-12-2002
		EP1350175 A1	08-10-2003
		EP1386268 A2	04-02-2004
		EP1413150 A2	28-04-2004
		EP1563421 A2	17-08-2005
		EP1599818 A2	30-11-2005
		EP1610897 A1	04-01-2006
		ES2215064T T3	01-10-2004
		ES2256037T T3	16-07-2006
		HK1047810 A1	11-08-2006
		HK1048550 A1	21-10-2004
		HR20020180 A2	30-06-2004
		HR20020197 A2	31-10-2004
		HU0202471 A2	28-11-2002
		HU0202700 A2	28-12-2002
		IL148319D D0	12-09-2002
		IL148320D D0	12-09-2002
		PL354415 A1	12-01-2004

PT1212732T T	30-06-2004
RU2252451 C2	20-05-2005
RU2265247 C2	27-11-2005
SI1212732T T1	31-10-2004
TR200201280T T2	21-08-2002
TR200201399T T2	21-11-2002
TR200202436T T2	21-01-2003
TW240209B B	21-09-2005
TW504647B B	01-10-2002
TW535078B B	01-06-2003
TW544605B B	01-08-2003
TW548564B B	21-08-2003
US6581839 B1	24-06-2003
US6742704 B2	01-06-2004
US6749123 B2	15-06-2004
US6764014 B2	20-07-2004
US6997378 B2	14-02-2006
US7035872 B2	25-04-2006
US7059531 B2	03-06-2006
US7070112 B2	04-07-2006
US7093767 B2	22-08-2006
US7119659 B2	10-10-2006
US7121471 B2	17-10-2006
US2001034720 A1	25-10-2001
US2002070279 A1	13-06-2002
US2002143626 A1	03-10-2002
US2002188509 A1	12-12-2002
US2002194068 A1	19-12-2002
US2003033211 A1	13-02-2003
US2003130895 A1	10-07-2003
US2003141373 A1	31-07-2003
US2003167207 A1	04-09-2003
US2003200144 A1	23-10-2003
US2004010449 A1	15-01-2004
US2004020992 A1	05-02-2004
US2004049451 A1	11-03-2004
US2004118930 A1	24-06-2004
US2004138989 A1	15-07-2004
US2004158532 A1	12-08-2004
US2004210448 A1	21-10-2004
US2004210449 A1	21-10-2004
US2004225602 A1	11-11-2004
US2004230488 A1	18-11-2004
US2004232220 A1	25-11-2004
US2004232221 A1	25-11-2004
US2004232222 A1	25-11-2004
US2004232224 A1	25-11-2004
US2004233037 A1	25-11-2004
US2004233038 A1	25-11-2004
US2004233039 A1	25-11-2004
US2004236699 A1	25-11-2004
US2004236700 A1	25-11-2004
US2004236701 A1	25-11-2004
US2004238620 A1	02-12-2004
US2004238621 A1	02-12-2004
US2004239480 A1	02-12-2004
US2004239481 A1	02-12-2004
US2004243468 A1	02-12-2004
US2004243520 A1	02-12-2004
US2004249839 A1	09-12-2004
US2004252012 A1	16-12-2004
US2004254835 A1	16-12-2004
US2004257197 A1	23-12-2004
US2004260646 A1	23-12-2004

US2005004866 A1	06-01-2005
US2005004921 A1	06-01-2005
US2005023359 A1	03-02-2005
US2005033619 A1	10-02-2005
US2005033686 A1	10-02-2005
US2005033687 A1	10-02-2005
US2005033689 A1	10-02-2005
US2005035192 A1	17-02-2005
US2005038718 A1	17-02-2005
US2005038736 A1	17-02-2005
US2005038741 A1	17-02-2005
US2005043992 A1	24-02-2005
US2005051633 A1	10-03-2005
US2005060233 A1	17-03-2005
US2005071231 A1	31-03-2005
US2005077349 A1	14-04-2005
US2005116810 A1	02-06-2005
US2005149544 A1	07-07-2005
US2005160003 A1	21-07-2005
US2005165695 A1	28-07-2005
US2005171898 A1	04-08-2005
US2005177499 A1	11-08-2005
US2005177500 A1	11-08-2005
US2005177501 A1	11-08-2005
US2005177502 A1	11-08-2005
US2005177503 A1	11-08-2005
US2005187883 A1	25-08-2005
US2005248459 A1	10-11-2005
US2006012473 A1	19-01-2006
US2006053056 A1	09-03-2006
US2006074698 A1	06-04-2006
US2006074813 A1	06-04-2006
US2006237528 A1	26-10-2006
US2006253329 A1	09-11-2006
WO0116900 A2	08-03-2001
WO0118745 A2	15-03-2001
WO0146902 A1	28-06-2001
WO0154082 A2	26-07-2001
WO0167355 A2	13-09-2001
WO0189924 A2	29-11-2001
WO02079925 A2	10-10-2002
WO03007623 A2	23-01-2003
WO2004006064 A2	15-01-2004
WO2004006162 A2	15-01-2004
WO2004006590 A2	15-01-2004
WO2004044825 A1	27-05-2004
WO2004079506 A2	16-09-2004
WO2005003903 A2	13-01-2005
WO2005086676 A2	22-09-2005
WO2005086721 A2	22-09-2005
WO2005086894 A2	22-09-2005
WO2005086897 A2	22-09-2005
WO2005086899 A2	22-09-2005
WO2005089132 A2	29-09-2005
WO2005089227 A2	29-09-2005
WO2005098737 A2	20-10-2005
WO2006012538 A2	02-02-2006
WO2006023198 A2	02-03-2006
WO2006026600 A2	09-03-2006
WO2006039180 A2	13-04-2006
WO2006044542 A2	27-04-2006
WO2006044553 A2	27-04-2006
ZA200202459 A	16-10-2002
ZA200202460 A	29-05-2003

Box No. V **Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1-78	YES
	Claims	None	NO
Inventive step (IS)	Claims	1-78	YES
	Claims	None	NO
Industrial applicability (IA)	Claims	1-78	YES
	Claims	None	NO

2. Citations and explanations :

The claimed invention relates to a method and apparatus for providing user authentication of a recipient unit when the recipient unit is off-line by storing one of a plurality of challenge-reply sets associated with an article based on an on-line communication with a sender unit.

The following documents appear in the International Search Report:

D1: US4795890; GOLDMAN, R. (03-01-1989)
D2: US2005/0033688; PEART et al. (10-02-2005)
D3: US2005/0144450; VOICE, C. (30-06-2005)

D1 discloses an authentication system for off-line authentication of cards during a controlled period of time whereby on-line verification is required to refresh the card for another period of off-line use [col. 2, lines 7-48]. A transaction device (card) stores time-related and holder specific data (magnetic stripe) which is used to regulate and validate the card and the cardholder by first and second level authentication processes [col. 3, lines 7-54], [col. 7, lines 13-29], [Figure 1].

D2 discloses a method and apparatus for a smartcard system to provide secure transaction completion in a contact or contactless environment using an RF proximity integrated circuit payment device by providing authentication data without intervention from the smartcard holder [Abstract], [0017]. The system comprises a smartcard in communication with a merchant smartcard or an RF reader communicating cardholder authentication and transaction authorization data. A merchant system retrieves information from the smartcard and determines if the transaction is to be performed on-line or off-line, whether there are any restrictions (risk factors) placed on the transaction account and which processing applications are supported by both the smartcard and the merchant system [0018], [0103]. D2 also discloses that the authentication may be performed using a "challenge/response" algorithm [0097], [0105] and, for off-line authentication, the merchant system authenticates the smartcard using static or dynamic authentication data (cryptogram), public/private key certificates and hash values to validate the card and cardholder [0107]-[0114].

D3 discloses a method and apparatus for providing mutual authentication between a user and a target resource using soft or hard tokens. A user possesses an article (card) having sender authentication data stored thereon and the method comprises determining the article's identification data (serial number or shared secret), sending a challenge which includes location information for the user to identify the desired sender authentication data located on the article [whole document].

The following observations were made:

Claims 1-63 are directed to a method and apparatus for providing user authentication of a recipient unit whereby the user can perform an off-line authentication using at least one successful challenge-reply set to access a particular resource available through the recipient unit based on an previous on-line communication with a sender unit and claims 64-78 are directed to a method, apparatus and system for providing user authentication of a recipient unit by matching at least one received reply to a challenge-reply set with a stored reply corresponding to the sent challenge.

(Continued on Supplemental Sheet)

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made :

Clarity

The following claims do not meet the requirements of **PCT Article 6**, since they are not clear and concise:

In claims 6, 29, 37, 54, 62 and 72, the expression "the challenge" lacks a proper antecedent.
In claims 7, 23, 30, 38, 55, 73 and 77, the expression "the number of stored challenge-reply sets" lacks a proper antecedent.
In claims 23, 29, 54, 72 and 77,the expression "the article" lacks a proper antecedent.
In claim 32, the expression "the sender unit" lacks a proper antecedent.
In claims 52 and 53, the expression "a request from the recipient unit" causes double inclusion.
Claim 66 is ambiguous since it is dependent upon claim 57 but should be made dependent on claim 65.

Disclosure

Page 20, [0080], line 7, the reference label "38" should be "14"
Page 25, [0092], line 14, the reference label "810" has been already assigned to the "server".
Page 27, [0096], line 18, the reference label "1402" should be "1302".
Page 39, [00124], line 1, the inclusion of the sentence "In addition use of the claim terms includes any representation thereof" is unclear.
Page 47, [00142,], line 3,the reference labels "2905" and "2920" should be "2406" and "2408" respectively.
Page 52, [00156], line 2, the terms "a the" should be replaced with "the".
Page 55, [00162], lines 19-20, the phrase "so that all of less than all" is unclear, the term "of" should be "or".
Page 56, [00165], line 9, the term "to" should be remoevd.

Figure 22, the reference label "32" pointing to the Internet/Intranet cloud should be removed.
Figure 24, in the text next to input line 32 to Box 2202, the term "user" is misspelled; the label "Y/N" linking Box 2406 and Box 2408 is unclear; the reference label "2402" associated with the database should be "2404" and the reference label "32" pointing to the Internet/Intranet cloud should be removed.
Figure 33, the reference labels "3305" and "3310" should be replaced with "2915" and "2920" respectively.

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**

Continuation of : Box V

Novelty

The present application describes a method, system and apparatus for providing user authentication of a recipient unit by matching at least one received reply to a challenge-reply set with a stored reply corresponding to the sent challenge and thereby the user can perform an off-line authentication using at least one successful challenge-reply set to access a particular resource available through the recipient unit based on an previous successful on-line communication with a sender unit.

Therefore the method, system and apparatus for providing user authentication of a recipient unit based on at least one received reply to a challenge-reply set thereby enabling a user to perform an off-line authentication, using the at least one successful challenge-reply set, to access a particular resource available through the recipient unit, as defined in claims 1-78, are considered novel in view of D1 thru D3 according to (**PCT Article 33(2)**).

Inventive Step

Claims 1- 78 are considered to have inventive step and meet the criteria set out in **PCT Article 33(3)** because the prior art D1 thru D3 do not explicitly teach a method, system and apparatus for providing user authentication of a recipient unit based on at least one received reply to a challenge-reply set thereby enabling a user to perform an off-line authentication, using the at least one successful challenge-reply set, to access a particular resource available through the recipient unit

Industrial Applicability

The subject matter of claims 1- 78 is considered to have industrial applicability and meet the criteria set out in **PCT Article 33(4).**